(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2002 (30.05.2002)

PCT

(10) International Publication Number
WO 02/43342 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US01/43615

(22) International Filing Date:
20 November 2001 (20.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/721,785 22 November 2000 (22.11.2000) US

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: **JARDIN, Cary, A.**; 12662 Sabre View Cove, San Diego, CA 92128 (US). **VARSANYI, Eric**; 4100 Ives Lane North, Plymouth, MN 55441 (US). **DUCLOS, Phil, J.**; 12968 Hillcrest Drive, Longmont, CO 80504 (US). **PADUA, Vincent, M.**; 13912 Capewood Lane, #296, San Diego, CA 92128 (US).

(74) Agent: **HARRIS, Scott, C.**; Fish & Richardson P.C., Suite 500, 4350 La Jolla Village Drive, San Diego, CA 92122 (US).

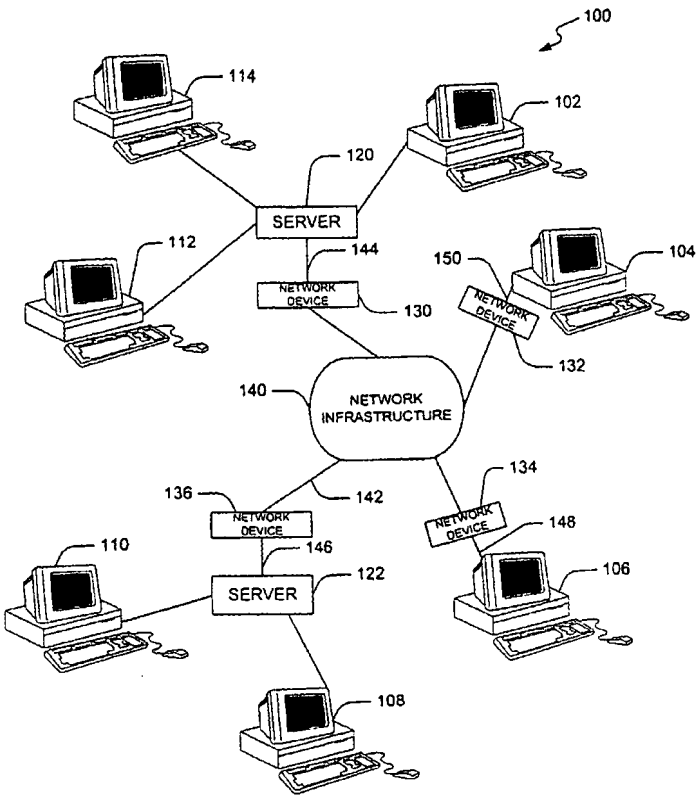
(81) Designated States *(national)*: BR, CN, IN, SG.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS



(57) Abstract: A link lock system for a network is disclosed. The system includes a computer, a network interface device, a bus monitor, and a security switch. The network interface device provides the computer with access to the network. The bus monitor monitors a link between the network interface device and the computer. The bus monitor reports detected failures or intrusions. The security switch switches the link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

WO 02/43342 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS

TECHNICAL FIELD

This invention relates to securing information across networks, and more particularly to monitoring and controlling a link between a network device and a computer for failures or intrusions.

BACKGROUND

The client/server model is often used to deliver information across a network. In this model, a client computer connects to a server on which information resides. The client computer may request the services of the server, such as delivering information. Other services may include searching for and sending back information, such as when a database on a network is queried.

A conceptual diagram of a computer network 100, such as the Internet, is illustrated in FIG. 1. The network 100 may comprise small computers 102-114 and large computers 120, 122, commonly used as servers. In general, small computers 102-114 are "personal computers" or workstations and are the sites at which a user operates the computer to

make requests for data from other computers or servers on the network 100.

A connection to the network 100 may be made through a network device 130-136 that provides an interface between the requesting computer (i.e. client) and the network infrastructure 140. The network device 130-136 may also be used to provide an interface between the network infrastructure 140 and the server 120, 122. The interface between the client 102-114, the server 120-122, and the network infrastructure 140 may be defined by a protocol referred to as the Hypertext Transfer Protocol (HTTP). The HTTP is the language that Web clients and servers use to communicate with each other. A secure version of this protocol, HTTP-S, is often used to provide communication between the network infrastructure 140 and the network device 130-136. However, the link between the network device 130-136 and the server 120-122, or the network device 130-136 and the small computer 102-114, is often configured in a non-secured mode.

DESCRIPTION OF DRAWINGS

These and other features and advantages of the invention will become more apparent upon reading the following detailed description and upon reference to the accompanying drawings.

Figure 1 is conceptual diagram of a computer network.

Figure 2 is a block diagram of a network system including a link lock system.

Figure 3 is a block diagram of a link lock system in accordance with an embodiment of the present disclosure.

Figure 4 illustrates a method for monitoring and controlling a link for failures or intrusions according to an embodiment.

DETAILED DESCRIPTION

The present disclosure includes a link-lock system coupled to the network device to monitor and control the security mode of a link between the network device and the server or the client. The security mode of the link may be controlled in accordance with the status of the link. For example, if a link failure or intrusion is detected, the security mode of the link is maintained in a secured state rather than converted into a non-secured state.

An embodiment of a network 200 having the link-lock system 206 is illustrated in FIG. 2. The network 200 includes a network interface device 204 configured to interface with the network infrastructure 201 through a link 202 operating in a secured protocol (e.g. HTTP-S). The HTTP-S provides a variety of security mechanisms to HTTP clients and servers, providing the security service options appropriate to wide range of potential end uses.

The network 200 further includes a link-lock system 206 coupled to the network interface device 204. The link-lock system 206 monitors security status of the link 208 between the network interface device 206 and a computer used to connect to the network, such as the server or the client 210. In the illustrated embodiment of FIG. 2, when the link-lock system 206 determines that a link failure or intrusion is detected, the security protocol of the link 208 is maintained in an HTTP-S mode rather than converted into an HTTP mode. The link failure or intrusion may include physical tampering or alteration of any part of the link 208 between the network interface device 204 and the server/client 210. The failure or intrusion may also include software attack or modification of the link 208 from external sources.

A block diagram of the link-lock system 206 in accordance with an embodiment of the present disclosure is shown in FIG. 3. The link-lock system 206 includes a bus

monitor 300, a security switch 302, an encryption/decryption element 304, and a controller 306. The link-lock system 206 may also maintain a protocol encryption element 308 on the server/client 210.

The security switch 302 receives data from the network interface device 204 or the server/client 210. In the illustrated embodiment, the security switch 302 commands the encryption/decryption element 304 to convert the received data from a secured protocol to a non-secured protocol, when the data is received from a network link 310 and is placed onto the link 208. The security switch 302 may command the encryption/decryption element 304 to convert the received data from a non-secured protocol to a secured protocol, when the data is received from the link 208 and is placed onto the network link 310. The converted data is then sent to the server/client 210 or the network interface device 204 using an appropriate protocol.

The bus monitor 300 monitors the link 208 for possible link failure or intrusion. When a link failure or intrusion is detected on the link 208, the bus monitor 300 notifies the controller 306. The controller 306, upon receipt of the link failure, directs the security switch 302 to keep the link 208 in a secured protocol mode. The controller 306 may also direct the protocol encryption element 308 in the server/client 210 to convert the data being placed on the link 208 using a secured protocol. In some embodiments, the

functions of the security switch 302, the bus monitor 300, and the controller 306 may be combined into a single element.

FIG. 4 illustrates a method for monitoring and controlling a link for failures or intrusions. The method includes monitoring the link between a network device and a server/client, at 400. When failures or intrusions are detected on the link, at 402, the link is directed to use a secured protocol at 404. Data sent across this link remains in a secured protocol mode until a network manager determines that the failures or intrusions have been corrected at 406.

Numerous variations and modifications of the invention will become readily apparent to those skilled in the art. Accordingly, the invention may be embodied in other specific forms without departing from its spirit or essential characteristics.

WHAT IS CLAIMED IS:

1. A link lock system for a network, comprising:

a computer;

a network interface device to provide the computer with access to the network;

a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions; and

a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

2. The system of claim 1, wherein said computer is a server.

3. The system of claim 1, wherein the network operates in a secured mode using an HTTP-S protocol.

4. The system of claim 1, wherein said non-secured mode of the first link between the network device and the computer uses HTTP protocol.

5. The system of claim 4, wherein said secured mode of the first link between the network device and the computer uses HTTP-S protocol.

6. The system of claim 1, further comprising:

a controller that receives the report from the bus monitor and sends control signals to the network interface device, the security switch, and the computer.

7. The system of claim 6, further comprising:

an encryption element in the computer, where said encryption element converts data placed on said first link to a secured protocol when the control signal is received from said controller.

8. A system for a server, comprising:

an interface device to provide the server with access to a network; and

a controller to monitor a link between the interface device and the server, where said controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link.

9. The system of claim 8, wherein the network is Internet, such that the non-secured protocol includes HTTP and the secured protocol includes HTTP-S.

10. The system of claim 8, wherein said controller sends a control signal to the server when failures or intrusions are detected on the link.

11. The system of claim 10, further comprising:

an encryption element in the server, where said encryption element converts data placed on said link by the server to a secured protocol when the control signal is received from said controller.

12. A method, comprising:

monitoring a link between a network device and a computer;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

13. The method of claim 12, wherein said non-secured protocol includes HTTP protocol.

14. The method of claim 12, wherein said secured protocol includes HTTP-S protocol.

15. The method of claim 12, wherein the computer is a server.

16. An apparatus comprising a machine-readable storage medium having executable instructions that enable the machine to:

monitor a link between a network device and a server;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

17. The apparatus of claim 16, wherein said non-secured protocol includes HTTP protocol.

18. The apparatus of claim 16, wherein said secured protocol includes HTTP-S protocol.

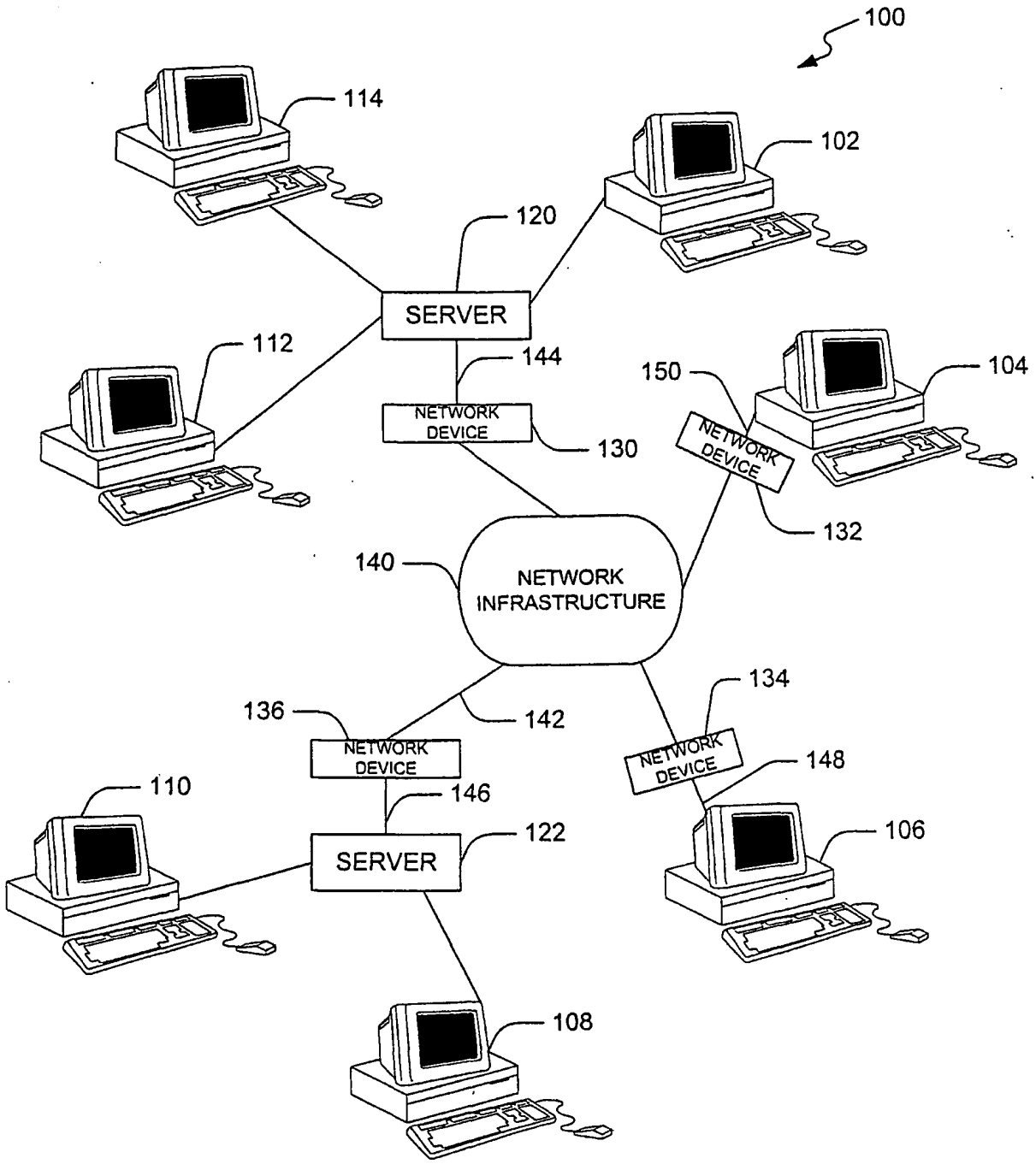


FIG. 1
(PRIOR ART)

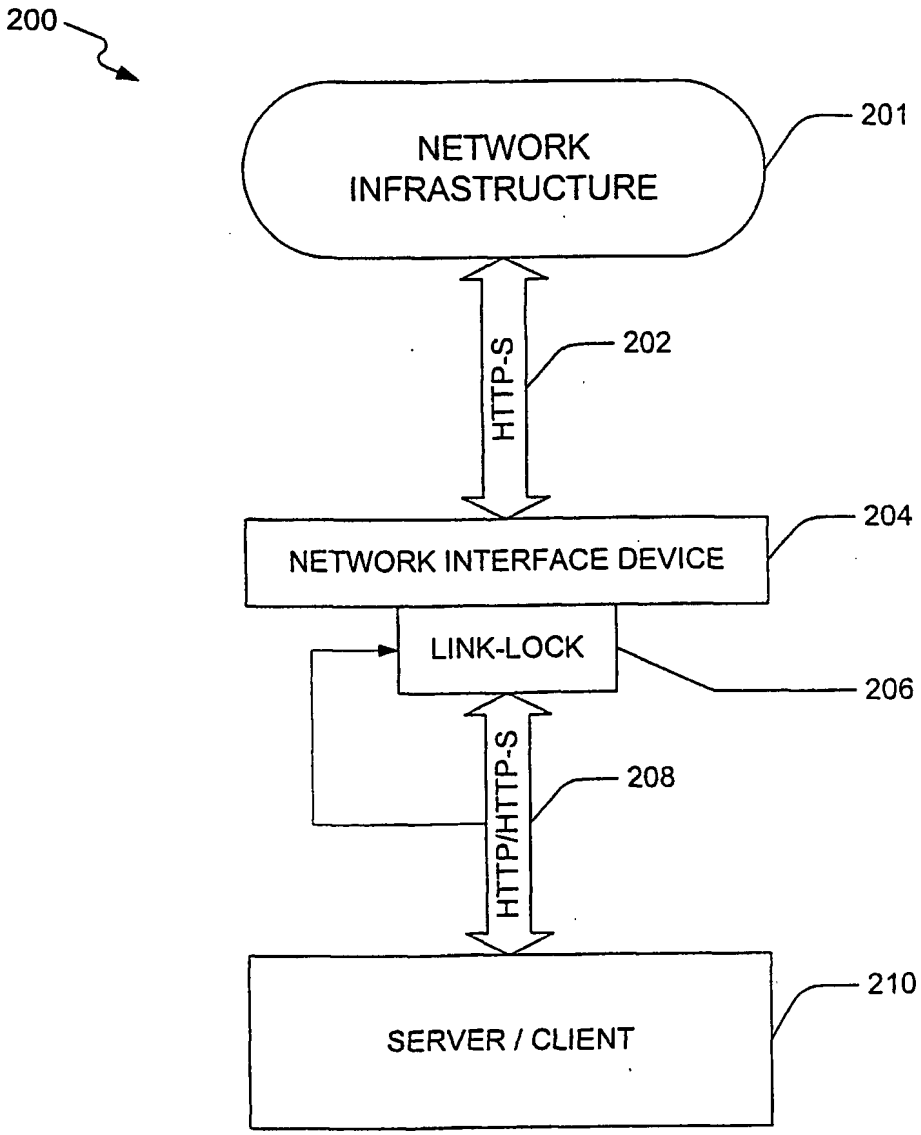

200
NETWORK INFRASTRUCTURE
201
HTTP-S
202
NETWORK INTERFACE DEVICE
204
LINK-LOCK
206
HTTP/HTTP-S
208
SERVER / CLIENT
210

FIG. 2

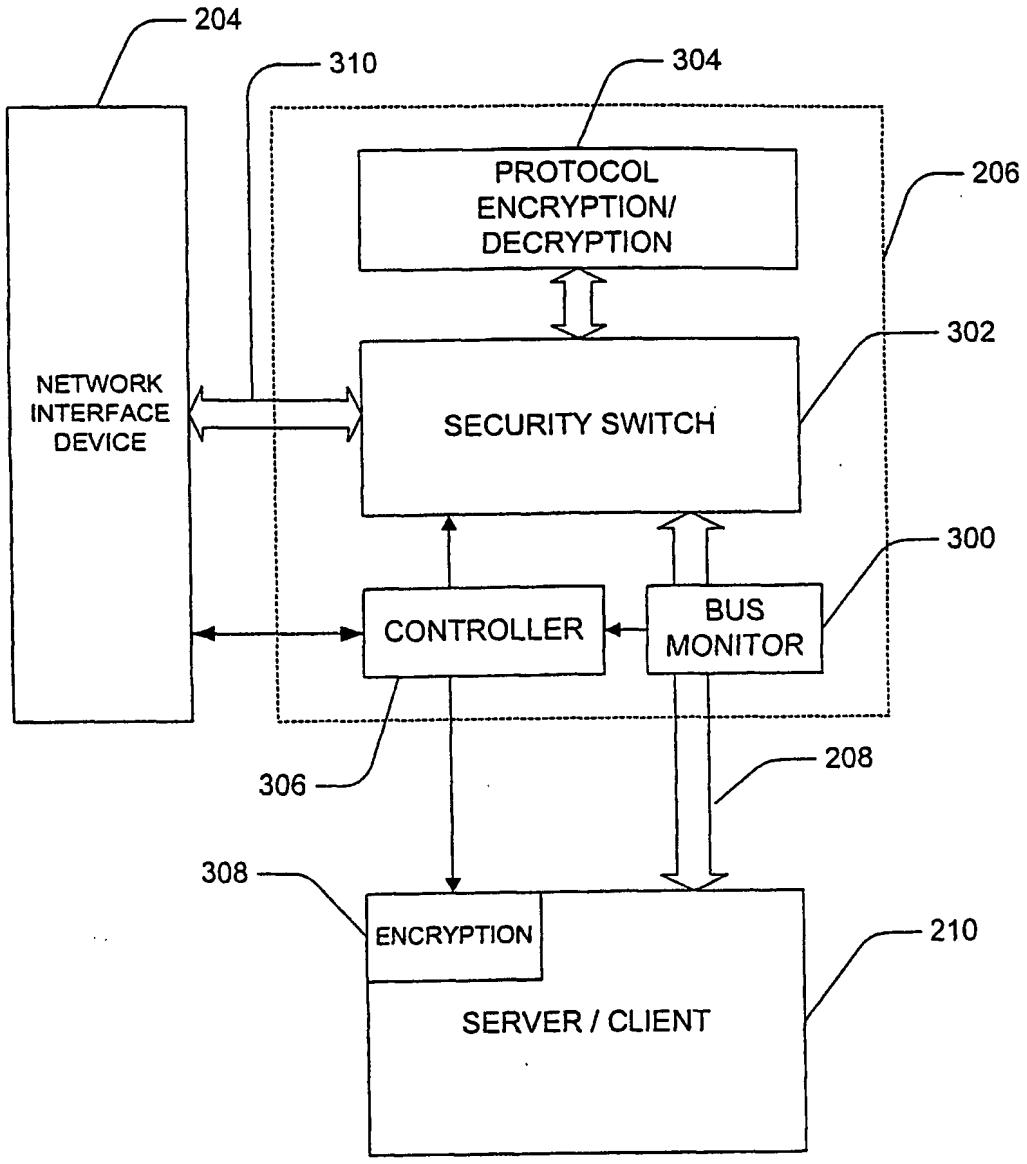

204
310
304
206
PROTOCOL ENCRYPTION/ DECRYPTION
NETWORK INTERFACE DEVICE
302
SECURITY SWITCH
300
CONTROLLER
BUS MONITOR
306
208
308
ENCRYPTION
210
SERVER / CLIENT

FIG. 3

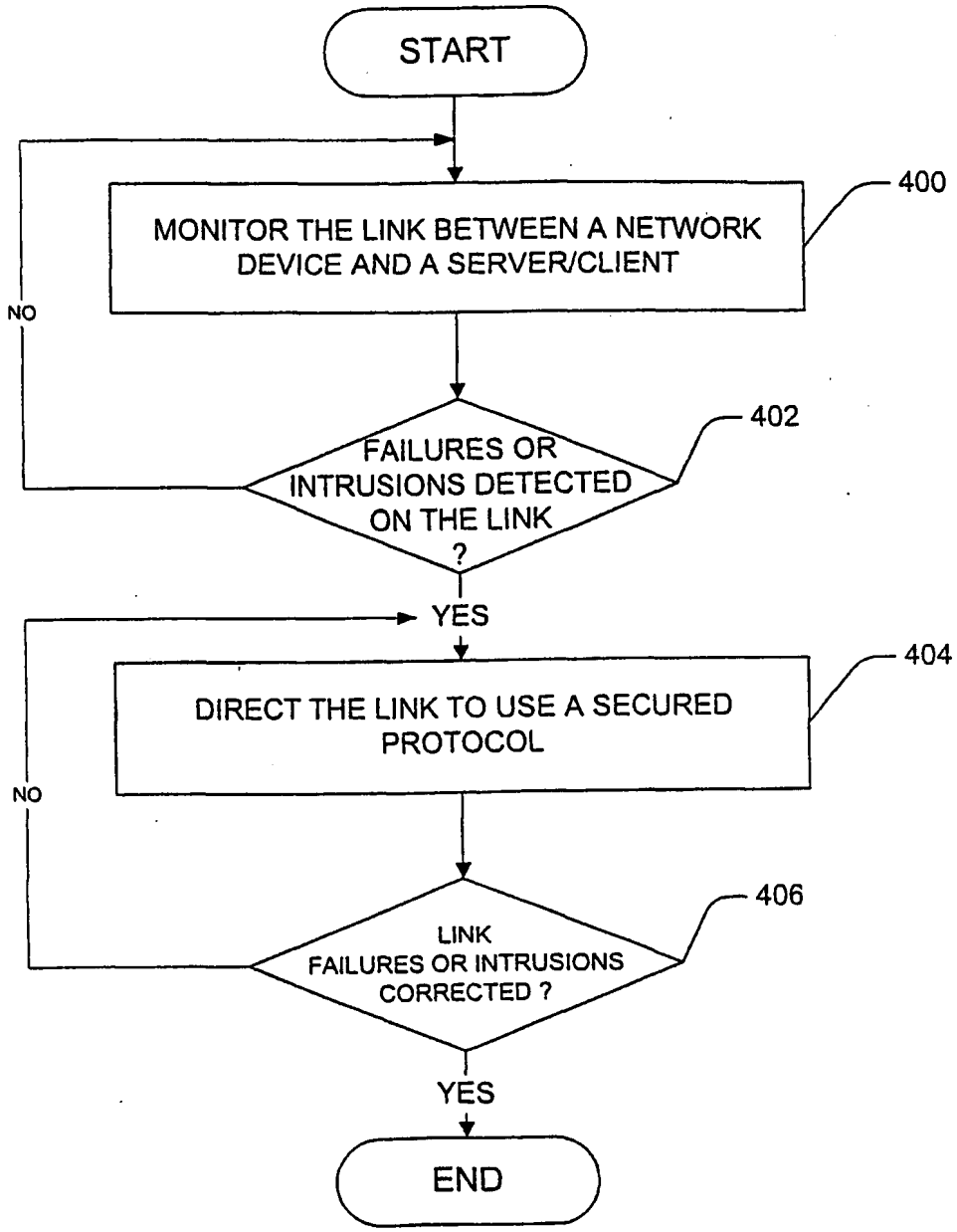

START
MONITOR THE LINK BETWEEN A NETWORK DEVICE AND A SERVER/CLIENT
400
FAILURES OR INTRUSIONS DETECTED ON THE LINK ?
402
NO
YES
DIRECT THE LINK TO USE A SECURED PROTOCOL
404
NO
LINK FAILURES OR INTRUSIONS CORRECTED ?
406
YES
END

FIG. 4